Information Assurance

Service Name: Information Assurance Level I

1. Service Description: Our sole mission is to protect and defend network availability, protect data integrity, and provide the ability to implement effective computer network defense for the Fort Detrick Network. The threat to telecommunications and IS throughout the Army is genuine and expanding. The increasing number of information resources result in an increased vulnerability to threats caused by both authorized users and through external attack. The reliance on information systems has made information technology a competitive weapon of unparalleled power and importance. The Department of Defense (DoD) has identified information and information resources as a priority target in future conflicts. As such, the simultaneous defense of our own information resources considered is just as critical. Therefore, it is the responsibility of all users to maintain Army operating standards and report any suspicious activities.

2. DOIM Responsibilities:

a. Coordinate the detection, correction, and reporting of malicious and unauthorized activities.
b. Implement and manage the Information Assurance Vulnerability Management (IAVM) program for all installation and tenant activities.
c. Perform network or workstation scans and compile vulnerability reports and corrections.
d. Provide written Certification and Accreditation statements (for example, Interim Approval to Operate/Connect (IATO/IATC)), and formal approval to operate (ATO) Certification and Accreditation documentation after formal review of SSAA and Certification and Accreditation documentation.
e. Develop and coordinate implementation of security procedures and protocols governing network operations.
f. Assist in the formal Information Assurance (IA) certification programs for Network Managers and Systems Administrators Information Technology Professionals; training for scanning personnel; and IA workstation/server implementation training/guidelines.
g. Implement and manage the IAVA program for all installation and tenant activities.

3. Customer Responsibilities: Army tenant units or activities must comply with the IA requirements of both their parent MACOM and the supporting installation. Army and non-Army tenant operations must comply with the host installation's IA policy if they connect to the installation's information infrastructure. Army tenant units or activities and units based in or under operational control (OPCON) of a MACOM other than their parent MACOM will comply with the IA requirements of both parent and host MACOMs. If a non-Army tenant uses any part of the host installation infrastructure, the installation IAM will require the use of configuration management controls consistent with the installation's information management and configuration management process. All tenant activities will —

a. Identify and coordinate all system upgrades, fielding, pilots, tests, and operations of new or upgraded systems with the installation IAM, DAA, and DOIM.

b. Identify ISS and provide the approved Certification and Accreditation documentation to the installation IAM.

c. Support installation IA efforts and requirements, and identify constraints in sufficient time to permit coordination and preparation of a viable IS security solution.

d. Coordinate and conduct vulnerability assessments or compliance scanning, and report completion and results as required.

4. Questions/Contact Information: If you have any questions or would like to obtain this service, please contact your Customer Account Manager (CAM) or check the DOIM web site at: http://doim.detrick.army.mil. If you do not know your CAM or your organization does not have a CAM assigned please contact the DOIM Help Desk at 301-619-2049 or via email at: *usagdoimhelpdesk@amedd.army.mil*.